CLAIMS

What is claimed is:

1. A method for validating a digital certificate within a data processing system, the method comprising:

receiving a digital certificate;

retrieving a certificate revocation list;

extracting a first serial number from the digital certificate, wherein the first serial number has been associated with the digital certificate by a certifying authority;

determining whether the first serial number matches a second serial number stored within the certificate revocation list;

in response to a determination that the first serial number matches the second serial number, computing a first certificate fingerprint for the digital certificate; and

comparing the first certificate fingerprint with a second certificate fingerprint stored within the certificate revocation list, wherein the second certificate fingerprint is associated with the second serial number.

2. The method of claim 1 further comprising:

in response to a determination that the first certificate fingerprint matches the second certificate fingerprint, invalidating the digital certificate.

3. The method of claim 1 further comprising:

in response to a determination that the first certificate fingerprint does not match the second certificate fingerprint, validating the digital certificate.

4. The method of claim 1 wherein the digital certificate and the certificate revocation list are formatted according to the X.509 standard.

5. The method of claim 1 wherein the second certificate fingerprint is stored within an X.509 extension within the certificate revocation list.

6. The method of claim 1 wherein the step of computing a first certificate fingerprint for the digital certificate uses a digest algorithm in accordance with a digest algorithm identifier stored in association with the second certificate fingerprint.

7. A method for revoking a digital certificate, the method comprising:

receiving a serial number for a digital certificate, wherein the serial number has been associated with the digital certificate by a certifying authority;

creating an entry in a certificate revocation list for the digital certificate, wherein the entry comprises the serial number for the digital certificate;

computing a certificate fingerprint for the digital certificate; and

storing the certificate fingerprint within the entry in the certificate revocation list for the digital certificate.

8. The method of claim 7 wherein the digital certificate and the certificate revocation list are formatted according to the X.509 standard.

9. The method of claim 7 wherein the certificate fingerprint is stored within an X.509 extension within the entry in the certificate revocation list for the digital certificate.

10. The method of claim 7 further comprising:

storing a digest algorithm identifier in association with the certificate fingerprint within the entry in the certificate revocation list for the digital certificate that identifies a digest algorithm that has been used to compute the certificate fingerprint.

11. An apparatus for validating a digital certificate within a data processing system, the apparatus comprising:

receiving means for receiving a digital certificate;

retrieving means for retrieving a certificate revocation list;

extracting means for extracting a first serial number from the digital certificate, wherein the first serial number has been associated with the digital certificate by a certifying authority;

determining means for determining whether the first serial number matches a second serial number stored within the certificate revocation list;

computing means for computing in response to a determination that the first serial number matches the second serial number, a first certificate fingerprint for the digital certificate; and

comparing means for comparing the first certificate fingerprint with a second certificate fingerprint stored within the certificate revocation list, wherein the second certificate fingerprint is associated with the second serial number.

12. The apparatus of claim 11 further comprising:

invalidating means for invalidating the digital certificate in response to a determination that the first certificate fingerprint matches the second certificate fingerprint.

13. The apparatus of claim 11 further comprising:

validating means for validating the digital certificate in response to a determination that the first certificate fingerprint does not match the second certificate fingerprint.

14. The apparatus of claim 11 wherein the digital certificate and the certificate revocation list are formatted according to the X.509 standard.

15. The apparatus of claim 11 wherein the second certificate fingerprint is stored within an X.509 extension within the certificate revocation list.

16. The apparatus of claim 11 wherein the computing means uses a digest algorithm in accordance with a digest algorithm identifier stored in association with the second certificate fingerprint.

17. An apparatus for revoking a digital certificate, the apparatus comprising:

receiving means for receiving a serial number for a digital certificate, wherein the serial number has been associated with the digital certificate by a certifying authority;

creating means for creating an entry in a certificate revocation list for the digital certificate, wherein the entry comprises the serial number for the digital certificate;

computing means for computing a certificate fingerprint for the digital certificate; and

first storing means for storing the certificate fingerprint within the entry in the certificate revocation list for the digital certificate.

18. The apparatus of claim 17 wherein the digital certificate and the certificate revocation list are formatted according to the X.509 standard.

19. The apparatus of claim 17 wherein the certificate fingerprint is stored within an X.509 extension within the entry in the certificate revocation list for the digital certificate.

20. The apparatus of claim 17 further comprising:

second storing means for storing a digest algorithm identifier in association with the certificate fingerprint within the entry in the certificate revocation list for the digital certificate that identifies a digest algorithm that has been used to compute the certificate fingerprint.

21. A computer program product in a computer readable medium for use in a data processing system for validating a digital certificate, the computer program product comprising:

instructions for receiving a digital certificate;

instructions for retrieving a certificate revocation list;

instructions for extracting a first serial number from the digital certificate, wherein the first serial number has been associated with the digital certificate by a certifying authority;

instructions for determining whether the first serial number matches a second serial number stored within the certificate revocation list;

instructions for computing, in response to a determination that the first serial number matches the second serial number, a first certificate fingerprint for the digital certificate; and

instructions for comparing the first certificate fingerprint with a second certificate fingerprint stored within the certificate revocation list, wherein the second certificate fingerprint is associated with the second serial number.

22. The computer program product of claim 21 further comprising:

instructions for invalidating the digital certificate in response to a determination that the first certificate fingerprint matches the second certificate fingerprint.

23. The computer program product of claim 21 further comprising:

instructions for validating the digital certificate in response to a determination that the first certificate fingerprint does not match the second certificate fingerprint.

24. The computer program product of claim 21 wherein the digital certificate and the certificate revocation list are formatted according to the X.509 standard.

25. The computer program product of claim 21 wherein the second certificate fingerprint is stored within an X.509 extension within the certificate revocation list.

26. The computer program product of claim 21 wherein the instructions for computing a first certificate fingerprint for the digital certificate uses a digest algorithm in accordance with a digest algorithm identifier stored in association with the second certificate fingerprint.

27. A computer program product in a computer readable medium for use in a data processing system for revoking a digital certificate, the computer program product comprising:

instructions for receiving a serial number for a digital certificate, wherein the serial number has been associated with the digital certificate by a certifying authority;

instructions for creating an entry in a certificate revocation list for the digital certificate, wherein the entry comprises the serial number for the digital certificate;

instructions for computing a certificate fingerprint for the digital certificate; and

instructions for storing the certificate fingerprint within the entry in the certificate revocation list for the digital certificate.

28. The computer program product of claim 27 wherein the digital certificate and the certificate revocation list are formatted according to the X.509 standard.

29. The computer program product of claim 27 wherein the certificate fingerprint is stored within an X.509 extension within the entry in the certificate revocation list for the digital certificate.

30. The computer program product of claim 27 further comprising:

instructions for storing a digest algorithm identifier in association with the certificate fingerprint within the entry in the certificate revocation list for the digital certificate that identifies a digest algorithm that has been used to compute the certificate fingerprint.

31. A data structure representing a certificate revocation list for use in a data processing system, the data structure comprising:

a serial number of a revoked digital certificate; and

a certificate fingerprint for the revoked digital certificate.

32. The data structure of claim 31 wherein the certificate revocation list contains a plurality of entries, wherein each entry corresponds to a revoked digital certificate, and wherein the serial number and the certificate fingerprint of the revoked digital certificate are stored within an entry.